

UNITED STATES DISTRICT COURT

for the
District of UtahFILED
2023 DEC 1 PM 12:14
CLERK
U.S. DISTRICT COURT

In the Matter of the Search of

*(Briefly describe the property to be searched
or identify the person by name and address)*

Case No. 4:23-mj-00203 PK

SAMSUNG CELL PHONE BEARING SERIAL NUMBER
359620/10/48285/3, CURRENTLY SECURED AT U.S.
PROBATION UNDER CASE GG07QR24GG0003

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:
See Attachment A.

located in the _____ District of _____ Utah _____, there is now concealed *(identify the person or describe the property to be seized)*:
See Attachment B.

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. 2252A(a)(5)	Possession of child pornography
18 U.S.C. 2252A(a)(2)	Receipt/distribution of child pornography

The application is based on these facts:
See attached Affidavit.

- ☐ Continued on the attached sheet.
☐ Delayed notice of _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

IVAN J
MURRAYDigitally signed by IVAN J
MURRAY
Date: 2023.12.01 10:08:34
-07'00'

Applicant's signature

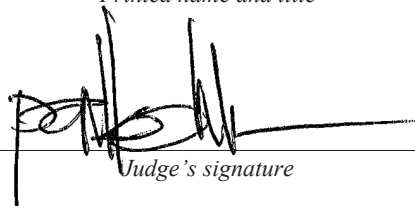
HSI SA Ivan Murray

Printed name and title

Sworn to before me and signed in my presence.

Date: 12/01/2023

City and state: St. George, Utah



Judge's signature

United Magistrate Judge Paul Kohler

Printed name and title

TRINA A. HIGGINS, United States Attorney (#7349)
CHRISTOPHER BURTON, Assistant United States Attorney (NV #12940)
Attorneys for the United States of America
Office of the United States Attorney
20 North Main Street, Suite 208
St. George, Utah 84770
Telephone: (435) 634-4270
Christopher.Burton4@usdoj.gov

IN THE UNITED STATES DISTRICT COURT

DISTRICT OF UTAH

IN THE MATTER OF THE
APPLICATION OF THE UNITED
STATES OF AMERICA FOR A
WARRANT AUTHORIZING THE
SEARCH OF A SAMSUNG CELL
PHONE BEARING SERIAL NUMBER
359620/10/48285/3, THAT IS
CURRENTLY SECURED IN THE
EVIDENCE ROOM AT U.S.
PROBATION AND PRETRIAL
SERVICES OFFICE LOCATED IN
SALT LAKE CITY, UTAH, UNDER
CASE NUMBER GG07QR24GG0003

AFFIDAVIT IN SUPPORT OF
APPLICATION FOR A SEARCH
WARRANT

Case No. 4:23-mj-00203 PK

AFFIDAVIT IN SUPPORT OF APPLICATION FOR A SEARCH WARRANT

I, Ivan Murray, Special Agent with Homeland Security Investigations, being duly
sworn, state:

AFFIANT BACKGROUND AND QUALIFICATIONS

1. I am a Special Agent with Homeland Security Investigations and have been
since November of 2011. I am currently assigned to assist the Federal Bureau of

Investigation's Child Exploitation Task Force (CETF) as well as the Utah Attorney General's Internet Crimes Against Children Task Force (ICAC). Prior to my current position with HSI, I was employed as a Criminal Investigator/Special Agent with Internal Revenue Service - Criminal Investigative Division for approximately seven years. I've received training in child-pornography investigations, and I've had the chance to observe and review numerous examples of child pornography (as defined in 18 U.S.C. § 2256) in all forms of media including computer media. I have received additional training from CETF and ICAC relating to online, undercover chatting investigations, as well as peer-2-peer or P2P investigations. While employed by HSI, I have investigated federal criminal violations related to high technology or cybercrime, child exploitation, and child pornography. Specifically, I have participated in numerous investigations relating to the sexual exploitation of children over the Internet since 2013.

PURPOSE OF AFFIDAVIT

2. I submit this Affidavit in support of an application for a search warrant for a Samsung cell phone, bearing serial number 359620/10/48285/3, that is currently secured in the evidence room at the U.S. Probation and Pretrial Services ("U.S. Probation) office located in Salt Lake city, Utah, Under case number GG07QR24GG0003 ("Subject Device").

3. This affidavit is intended to show merely that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter. The facts in this affidavit are included based on my training and experience, as well as my review of reports written by other law enforcement officers.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of Title 18 U.S.C. § 2252A(a)(5) (Possession of child pornography) and 18 U.S.C. § 2252A(a)(2) and (b)(1), (Receipt of child pornography) have been committed by BRADLEY THOMAS (the “Target Offenses”). There is also probable cause to search the Subject Device described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of the Target Offenses as further described in Attachment B.

SEARCH METHODOLOGY TO BE EMPLOYED

5. The search procedure of electronic data contained in computer hardware, computer software, and/or memory storage devices may include the following techniques (the following is a non-exclusive list, as other search procedures may be used):

a. examination of all of the data contained in such computer hardware, computer software, and/or memory storage devices to view the data and determine whether that data falls within the items to be seized as set forth herein;

b. searching for and attempting to recover any deleted, hidden, or encrypted data to determine whether that data falls within the list of items to be seized as set forth herein (any data that is encrypted and unreadable will not be returned unless law enforcement personnel have determined that the data is not (1) an instrumentality of the offenses, (2) a fruit of the criminal activity, (3) contraband, (4) otherwise unlawfully possessed, or (5) evidence of the offenses specified above);

c. surveying various file directories and the individual files they contain;

d. opening files in order to determine their contents;

e. using hash values to narrow the scope of what may be found. Hash values are used to find previously identified files of images of child pornography and do not capture images that are the result of new production, images embedded in an alternative file format, or images altered, for instance, by a single pixel. Thus, hash value results are under-inclusive, but are still a helpful tool;

f. scanning storage areas;

g. performing key word searches through all electronic storage areas to determine whether occurrences of language contained in such storage areas exist that are likely to appear in the evidence described in Attachment A; and/or

h. performing any other data analysis technique that may be necessary to locate and retrieve the evidence described in Attachment B.

BACKGROUND REGARDING DIGITAL DEVICES

6. Based upon my training, my experience, and my discussions with other law enforcement agents, I know the following:

a. Users of digital devices increasingly choose to store items in digital form (e.g. pictures, documents) because digital data takes up less physical space, and can be easily organized and searched. Users also choose to store data in their digital devices, such as cell phones, because it is more convenient for them to access data in devices they own, rather than to later spend time searching for it. Keeping things in digital form can be safer because data can be easily copied and stored off site as a failsafe.

b. Users also increasingly store things in digital form because storage continues to become less expensive. Today, 500 gigabyte (GB) hard drives are not

uncommon in computers. As a rule of thumb, users with 1 gigabyte of storage space can store the equivalent of 500,000 double spaced pages of text. Thus, each computer can easily contain the equivalent of 250 million pages, that, if printed out, would fill three 35' x 35' x 10' rooms. Similarly, a 500 GB drive could contain 450 full run movies, or 450,000 songs, or two million images. With digital devices, users can store data for years at little or no cost.

c. Storing data in digital form and not deleting it mirrors users' online habits where users have, for years, been encouraged to never delete their E mails. For example, on March 27, 2007, Yahoo! Mail announced free, "unlimited" capacity that gave their users "the freedom to never worry about deleting old messages again." See <[http://ycorpblog.com/2007/03/27/yahoo mail goes to infinity and beyond/](http://ycorpblog.com/2007/03/27/yahoo%20mail%20goes%20to%20infinity%20and%20beyond/)> (accessed April 18, 2012). Similarly, since June 2007, Google, Inc. has promoted free, increasingly larger storage "so you should never have to delete mail." <[http://gmailblog.blogspot.com/#!/2007/06/welcome to official gmail blog.html](http://gmailblog.blogspot.com/#!/2007/06/welcome%20to%20official%20gmail%20blog.html)>; see also <[http://gmailblog.blogspot.com/2007/10/more gmail storage coming for all.html](http://gmailblog.blogspot.com/2007/10/more%20gmail%20storage%20coming%20for%20all.html)> (accessed April 18, 2012) (promoting its "Infinity+1" plan to constantly give subscribers more storage). Hotmail also has advertised free, "virtually unlimited space," noting that "Hotmail gives you all the space you need." See <<http://www.microsoft.com/windows/windowslive/anotherlookathotmail/storage/>> (accessed April 18, 2012).

d. Digital devices can also store data automatically, without a user's input. For example, network logs may track an employee's actions for company auditing

purposes or E mail headers may automatically list the servers which transmitted the E mail. Similarly, a web browser (i.e. an application such as Internet Explorer used to access web pages) can track a user's history of websites visited so users can more easily re access those sites. Browsers also often temporarily cache files from recently accessed web pages to improve the user's experience by reducing that page's loading time. These examples illustrate how the interaction between software and operating systems often results in data being stored without a user's knowledge. Even if a sophisticated user understands this automatic storage of data, attempts at deleting this data often fail because the data may be automatically stored multiple times and in different locations. Thus, digital evidence may exist despite attempts at deleting it.

e. Digital data is particularly resilient to deletion. First, as noted, data is often automatically stored multiple times in multiple places, where even sophisticated users may not be able to locate. Second, digital data can be recovered years after it has been saved, or viewed B even after such data has been deleted. For example, when a user deletes a file on a computer, the file is sent to the recycle bin, where it can still be retrieved. Even if the file is deleted from the recycle bin, the data does not actually disappear; rather, it remains in "free space" or "slack space" (i.e. in unused space) until it is overwritten by new data. Third, an operating system may also keep deleted data in a "recovery" or "swap" file. Fourth, files from websites are automatically retained in a temporary cache, which are only overwritten as they are replaced with more recently viewed web pages. Thus, the ability to retrieve residues of an electronic file from a hard drive depends less on when the file was

downloaded or viewed than on a particular user's operating system, storage capacity, and computer use habits.

DETAILS OF THE INVESTIGATION

7. In 2015, BRADLEY JAMES THOMAS (hereafter, "THOMAS") was indicted on federal charges of 18 U.S.C. § 2252A(a)(5)(B), Possession of Child Pornography and 18 U.S.C. § 2252A(a)(2) and (b)(1), Receipt of Child Pornography. In 2016, THOMAS pleaded guilty to one count of Possession of Child Pornography and was subsequently ordered to serve 60 months in prison. Following his prison term, THOMAS was ordered to serve a term of supervised release for a period of 120 months. Beginning February 27, 2020, this 120-month period of supervision was initiated by U.S. Probation.

8. Per the terms of THOMAS' supervised released conditions, THOMAS is subject to "standard conditions" as well as "special conditions" that he must follow in order to be in compliance. Generally, officers of the U.S. Probation refer to these conditions when determining whether or not a probationer/ward under their supervision is compliant with these terms.

9. In reviewing the "Standard Conditions" of THOMAS' Terms of Supervised Release (hereafter, "SR"), I observed numerous conditions THOMAS is subject to. Specifically, SR paragraph 14 reads:

You must submit your person, residence, office or vehicle to search, conducted by the probation office as (SIC) a reasonable time and in a reasonable manner based upon reasonable suspicion of contraband of a violation of a condition of release; failure to submit to a search may be grounds for revocation; you must warn any other residents that the premises may be subject to searches pursuant to this condition.

10. In reviewing the Special Conditions of THOMAS' SR, I observed numerous conditions THOMAS is subject to. Specifically, SR paragraph 4 reads:

The defendant shall participate in the United States Probation and Pretrial Service Office Computer and Internet Monitoring Program under a co-payment plan and will comply with the provisions outlined in: Appendix A (discussed below), Monitored Computer Access. Furthermore, all computers, networks, Internet accessible devices, media storage devices, and digital media accessible to the defendant are subject to manual inspection/search, configuration, and the installation of monitoring software and/or hardware.

11. In reviewing the associated Appendix A, "Computer and Internet Monitoring Program Agreement," I observed numerous conditions THOMAS is subject to. Specifically, paragraph 5 reads:

If the court has not prohibited my use or possession of a computer, I understand that I may only use computer(s) in my home or at my place of employment that have been approved by the USPO. I further understand I am responsible for the content, programs, and data that may be stored or accessed by a computer I am permitted to use.

SUPERVISED RELEASE VIOLATED

12. On September 13, 2023, U.S. Probation Officer Adam Foster filed a Petition and Order for Warrant for Person Under Suspicion with the United States District Court for the District of Utah. In the petition, Officer Foster listed four alleged violations of THOMAS' SR. The allegations included failing to submit to drug testing, failing to refrain from using controlled substances, and engaging in other acts in violation of federal, state, or local crimes.

13. On September 13, 2023, the warrant issued for alleged violations of THOMAS' SR which was then forwarded to the United States Marshal Service (USMS)

for execution of the order. Around that time, THOMAS was suspected of being present inside of his parents' residence located at 787 North 1700 East St. George, Utah. USMS and U.S. Probation officers subsequently affected the arrest warrant and took THOMAS into custody.

14. After placing THOMAS in custody, THOMAS stated he was in possession of one mobile device located in a lower-level bedroom of the residence (parents' residence). This mobile device was subsequently retrieved and identified as a Samsung Galaxy S21, Model SM-G991U (Not the Subject Device relating to this affidavit). U.S. Probation agents then asked THOMAS if any illegal images would be found on this device to which THOMAS replied in the negative.

15. Agents then inquired of THOMAS as to what they might find if they conducted a search of his residence located at 445 West River Willow Lane Washington, Utah. THOMAS replied that agents would find ammunition in a lock box located in the master bedroom. USMS then read THOMAS his *Miranda* warnings and THOMAS was transported to the Washington County Detention Center.

16. After THOMAS was taken from the scene, a U.S. Probation agent placed a phone call to THOMAS' wife and directed her to meet U.S. Probation agents at THOMAS' residence located at the River Willow Lane address. Upon arrival of THOMAS' wife and U.S. Probation personnel at THOMAS' residence, a search of the residence ensued. Officers present did locate the ammunition identified by THOMAS. A search of a coat closet located in the living room of the residence revealed the presence of a mobile device positioned on the top shelf. The phone was later identified as a Samsung Galaxy model

SM-A102U bearing serial number 359620/10/48285/3 (“Subject Device”). Probation had no prior knowledge of THOMAS’ possession of the Subject Device. The Subject Device was booked into evidence at the U.S. Probation office and was later shipped to U.S. Probation offices located in Salt Lake City, Utah for further examination.

17. On October 3, 2023, U.S. Probation Forensic Agent Matt Birnbaum attempted to forensically extract the Subject Device pursuant to THOMAS’ search condition; however, due to the Subject Device being electronically secured (passcode encrypted), Forensic Agent Birnbaum deployed Cellebrite Premium (a forensic software tool) on the Subject Device in an effort to extract the device. Cellebrite Premium was successful in unlocking the device and revealed the passcode. Birnbaum was then able to perform a full File System extraction of the Subject Device.

18. Following the successful extraction of the Subject Device, U.S. Probation Officer Frank Davis analyzed the File System extraction from the Subject Device. Officer Davis observed significant evidence of communications between THOMAS and other individuals. Additionally, Davis observed several images of THOMAS’ child as well as cartoon figures (aka Anime) depicting child pornography. A further review of the extraction revealed a video file depicting child pornography. Much of the material located on this device violated the conditions of THOMAS’ SR.

REVIEW OF THE APPARENT CHILD PORNOGRAPHY

19. Due to the possible *criminal* violations committed by THOMAS while utilizing the Subject Device, I was invited to evaluate the findings of U.S. Probation with regards to the Subject Device. While it is appropriate and lawful for U.S. Probation to

report their criminal findings to the appropriate policing entity, receiving entities are necessarily obligated to independently investigate and verify any allegation independently from U.S. Probation. Despite this independence, I was obligated to review a minimal amount of information produced by U.S. Probation in order to justify my criminal probe of THOMAS' activities.

20. While I have reviewed some of the extraction of the Subject Device conducted by personnel from U.S. Probation, including viewing a video of apparent child pornography referenced above, I have not viewed the full Subject Device extraction in its entirety. However, the video file of apparent child pornography recovered by U.S. Probation is significant insofar as it helps to establish probable cause for a search of the Subject Device. As such, I have reviewed the file and I describe it as follows:

MP4 File Name: 5575ffdc-2406-4a3b-b97a-8ce5fbd1351c

Video Length: 28 seconds

Description: The video depicts a Caucasian female, approximately 11 years of age, facing the camera while wearing a peach-colored hoodie. She is then observed standing up and turning her back to the camera. She then removes her underwear and bends forward exposing her anus and genitals. She then places her hand near her buttocks and inserts one of her fingers into her anus. She continues to manipulate her anus and surrounding areas with her fingers.

///

///

///

///

///

CONCLUSION

21. Based on the facts set forth in this affidavit, I respectfully submit that there is probable cause to believe that the Subject Device contains evidence of Title 18 U.S.C. § 2252A(a)(5) (Possession of child pornography) and 18 U.S.C. § 2252A(a)(2) and (b)(1), (Receipt of child pornography) and that the information sought herein will materially aid the investigation.

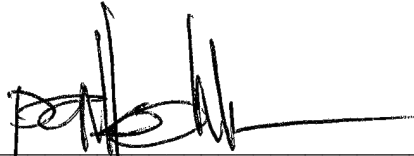
RESPECTFULLY SUBMITTED this 1st day of December, 2023.

IVAN J MURRAY

Digitally signed by IVAN J
MURRAY
Date: 2023.12.01 10:07:16 -0700'

Ivan Murray, Special Agent
Homeland Security Investigations

Subscribed and sworn to before me this 1st day of December, 2023.



JUDGE PAUL KOHLER
United States Magistrate Judge

ATTACHMENT “A”
Property to Be Searched

The Subject Device is described as a Samsung cell phone, bearing serial number 359620/10/48285/3, and any SIM card contained therein, that is currently secured at the evidence room located at the U.S. Probation and Pretrial Services Office located in Salt Lake City, Utah under case number GG07QR24GG0003.

ATTACHMENT B
LIST OF ITEMS TO BE SEARCHED FOR AND SEIZED

This affidavit is in support of application for a warrant to search a Samsung cell phone bearing serial number 359620/10/48285/3, and any SIM card contained therein, which is more specifically identified in the body of the application and in Attachment A (“Subject Device”), that can be used to store information and/or connect to the Internet, or which may contain mobile devices, for records and materials that are fruits, evidence, or instrumentalities of violations of Title 18, United States Code, Sections Title 18 U.S.C. § 2252A(a)(5), and 18 U.S.C. § 2252A(a)(2) and (b)(1) (“Target Offenses”). These records and materials are more specifically identified as:

1. Any and all computer software, including programs to run operating systems, applications (like word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs;
2. Any computer-related documentation, which consists of written, recorded, printed or electronically stored material that explains or illustrates how to configure or use computer hardware, software or other related items;
3. Any and all records and materials, in any format and media (including, but not limited to, text messages, SMS messages, picture/video messages, social media communication, envelopes, letters, papers, e-mail, chat logs and electronic messages), pertaining to the Target Offenses;
4. Records and information evidencing occupancy or ownership of the Subject Device described above, including, but not limited to, sales receipts, registration records,

records of payment for Internet access, usernames, passwords, device names, and records of payment for access to newsgroups or other online subscription services;

5. Stored electronic data and related digital storage relating to Global Positioning System (“GPS”) data;

6. Records evidencing the use of the Subject Device’s capability to access the Internet, including: records of Internet Protocol addresses used and records of Internet activity, including firewall logs, caches, browser history and cookies, “bookmarked” or “favorite” web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses;

7. Images and videos, to include any metadata identifying the date and location of the Subject Device at the time of the photo or video pertaining to the Target Offenses;

8. Evidence of who used, owned, or controlled the Subject Device at the time the things described in this warrant were possessed, accessed, received, created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;

9. Evidence of software that would allow others to control the Subject Device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software; and evidence of the lack of such malicious software;

10. Evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the Subject Device;

11. Evidence of the times the Subject Device was used;
12. Passwords, encryption keys, and other access devices that may be necessary to access the Subject Device.